



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

ESSAY

RATIONALIZATION AND INTERNAL CONTROL

Improving Marine Corps Unit-Level Internal Management Controls
for the Government-Wide Commercial Purchase Card Program

by:

Lewis E. Wood

December 2003

Thesis Advisors:

Donald Summers
Juliette Webb

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE DEC 2003		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Rationalization and Internal Control Improving Marine Corps Unit-Level Internal Management Controls for the Government-Wide Commercial Purchase Card Program				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Lewis E. Wood				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School, Monterey, CA				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 14	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

RATIONALIZATION AND INTERNAL CONTROL

Improving Marine Corps Unit-Level Internal Management Controls for the Government-Wide Commercial Purchase Card Program

"The General Accounting Office (GAO) has uncovered what may be the tip of the iceberg with regard to improper purchases by people empowered to buy using their government-wide purchase cards..."¹

Numerous newspaper articles and other reports echoing the issue highlighted by the preceding quote, coupled with other documents such as the Marine Corps' semi-annual review of its Government-wide Commercial Purchase Card (GCPC) Program for the first half of fiscal year (FY) 2003, led the author of this article to review GCPC usage in the Marine Corps as the basis for a Naval Postgraduate School Master of Business Administration thesis. The following paragraphs are a summation of the analysis made in that thesis by the author and Lieutenant Colonel Robert J. Darling, USMC. Although the GCPC program has proven to be of tremendous value to the Department of Defense (DoD), it has also experienced high levels of fraud, waste, and abuse. Many of the difficulties DoD has experienced with the GCPC program are results of weaknesses in the program's internal control environment. The recommendations in this article are offered as a means to improve that environment.

The Government-Wide Commercial Purchase Card Program

All federal agencies, including all components of the DoD, use the GCPC to make "micro-purchases" (purchases less than \$2,500) from commercial vendors. Although the cards can be used along with other contracting methods to pay for purchases up to \$9,999,900,² they are used extensively to buy low-dollar value items while avoiding the longer and more costly traditional acquisition process. The simplification of the purchasing process provided by the GCPC program has sped delivery of low-dollar value items to end users while also lowering the direct costs associated with making those purchases. Unfortunately, the program has also experienced significant shortcomings in its internal control environment.

The GCPC program grew out of the 1982 Presidential Executive Order 12352, *Procurement Reform*, which directed the DoD, as well as all executive agencies, to "Establish programs to simplify small purchases" along with other initiatives

1. <http://www.managementconcepts.com/acquisition/NavyCardarchive.asp>, 24 Oct 03.

2. EBUSOPSOFFINST 4200.1A, p. 1.

intended to streamline and simplify various governmental procurement processes.³ On July 6, 1998, the Department of the Navy (DoN) awarded a three-year contract (with options for extending the service period) to Citibank to provide purchase card services throughout the DoN.⁴ Currently managed by the DoN eBusiness Operations Office (EBUSOPSOFF), the program is part of the U.S. General Services Administration's (GSA) "SmartPay" program, whose current contracts with five service providers (Bank of America, Bank One, Citibank, Mellon Bank, and U.S. Bank) are effective until November 29, 2003.⁵

According to the executive summary of the June 27, 2002 DoD Charge Card Task Force Final Report, implementation of the GCPC program had resulted in an estimated savings of \$900 million by the report date.⁶ The GCPC program generates these savings in two ways: 1) as a result of cost reductions from the automation and streamlining of purchase order processes; and 2) from rebates from card issuers based on volume of transactions.

The automation and streamlining of the acquisition process save the DoD an estimated \$20 for every item purchased with the card as compared to the former, strictly paper-based, approval-laden buying process.⁷ In 2002, GCPC cardholders made more than ten million purchases with their cards, saving the government in excess of \$200 million in administrative costs. As stated by Under Secretary of Defense (Comptroller) and Chief Financial Officer Dov S. Zakheim at a June 27, 2002 press conference in regards to GCPC program cards, "...they really are essential to improving business practices."⁸

In addition to saving the government money by automating and streamlining the acquisition process, card-issuing banks provide the government with cash rebates or refunds for early or on-time payment of bills. The rebate or refund computation formula is included in the purchase card contract; the card issuer calculates the amount on a monthly basis for all purchases made with DoD GCPC program cards, and that calculation is verified by the Defense Finance and Accounting Service (DFAS). Rebates or refunds attributable to the use of the government purchase cards are credited to operation and maintenance (O&M) accounts of the DoD. Although individual military units or DoD organizations do not receive the rebates themselves, which would have the effect of increasing their O&M purchasing power, the

3. Executive Order 12352, 17 Mar 1982.

4. <http://www.don-ebusiness.navsup.navy.mil>, 30 Oct 2003.

5. <http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8199&channelPage=%2Fep%2Fchannel%2FgsaOverview.jsp&channelId=-13497>, 31 Oct 2003.

6. 2002 DoD Charge Card Task Force Final Report, p. v.

7. 2002 DoD Charge Card Task Force Final Report, p. 2-1.

8. Defense Link, *DoD Moves to Improve Charge Card Programs*, 27 Jun 2002.

savings to DoD can be substantial. Figure 1 shows the FY-03 rebate savings amounts calculated (in thousands) through September 2003.

GCPC Program Management

For the DoN, including the Marine Corps, EBUSOPSOFF Instruction (EBUSOPSOFFINST) 4200.1A is the current instruction which outlines GCPC program management procedures and responsibilities. The GCPC program is administered under the hierarchical structure depicted in Figure 2. At the lowest level of the GCPC program is the actual GCPC cardholder. Next is the Approving Official (AO), responsible for approving the cardholder's purchases and certifying monthly invoices from Citibank. The unit-level (level five) Agency Program Coordinator (APC) supervises the entire unit's GCPC program for the Head of Activity (HA), normally the unit's Commanding Officer. Above the HA are additional APC levels, individuals responsible for coordinating an ever-broadening scope of the GCPC program, up to the Major Claimancy level (level three).

Training for all GCPC program participants can be accomplished on-line and consists of a minimum of two parts. Training tailored to individual roles within the GCPC program is offered on the Navy's e-Business website; additionally, GCPC program participants must take the GCPC program tutorial offered through the Defense Acquisition University Continuous Learning Center.

Once training is completed, DoN GCPC program participants are required to adhere to the program administration rules outlined in the EBUSOPSOFFINST 4200.1A. AOs can supervise up to seven separate cardholder accounts and are responsible for overseeing and auditing those accounts, while a level five APC can be assigned to oversee up to three hundred individual cardholder accounts. Once a cardholder has been officially assigned as such by his HA, an APC sets up the cardholder's account with Citibank, normally on-line, and the cardholder then receives a GCPC program card directly from Citibank. The unit APC also ensures cardholders and AOs attend required refresher training, facilitates the issuance of the card to the cardholder, and sets the cardholder's single purchase and monthly transaction limits, as designated by the HA.

GCPC program cards are issued individually to cardholders and, although stating that the card is to be used only for official U.S. Government purchases, bear the cardholder's name. The cardholder is responsible for making only approved purchases with the card and bears pecuniary liability to the U.S. Government for illegal purchases. The cardholder is also

responsible to review mandatory sources of supply (in accordance with the Javits-Wagner-O'Day Act Program (JWOD), by screening items available from the Federal Prison Industries (FPI), and per the Resource Conservation and Recovery Act), to reconcile monthly billing statements from Citibank, act to resolve any discrepancies in those statements, and to certify monthly invoices for payment.

AOs approve cardholder purchases, verify the monthly statements for each of their cardholders, and forward their certifications of those statements to the DFAS. Upon AO certification of a cardholder's monthly statement, DFAS pays Citibank for the validated transactions.

Level five APCs perform a number of responsibilities in addition to overseeing the training of cardholders and AOs. APCs manage the issuance of GCPC cards within their units, coordinate with higher-level APCs, monitor the activities of their AOs and cardholders, and coordinate with Citibank when necessary to help resolve discrepancies. They conduct monthly transactional reviews of the purchases of all their subordinate cardholders, attempting to identify any questionable card activity for additional investigation. They also ensure the accuracy of their cardholder account profiles at least quarterly and are responsible to conduct semi-annual reviews of the functioning of their local programs.

In addition to these administrative personnel, EBUSOPSOFFINST 4200.1A specifies that a unit Review Official (RO) audit AO certifications monthly using stratified statistical random sampling methods. If at all possible the RO, although a member of the same unit as the AO and cardholder, is not to be a member of the AO's supervisory chain-of-command. The RO's function is to provide an additional screen to help ensure the validity of cardholder purchases and the timeliness of cardholder and AO certifications.

Fraud, Waste, and Abuse

As highlighted in the DoD Charge Card Task Force Final Report of June 27, 2002 and the October, 2002 GAO testimony on Navy purchase card vulnerabilities, significant weaknesses have existed in GCPC program internal control throughout the DoN (as shown in numerous other audits and internal investigations) as well as the DoD and other federal agencies. These weaknesses, which include lack of adherence to key internal controls and shortcomings in the GCPC program's management culture and supporting infrastructure,⁹ have drawn increasing managerial attention within the department since implementation of the program. In recent years, efforts to improve the GCPC program internal control environment appear to have focused principally on developing better means to identify fraud and other card misuse.

In addition to improved fraud identification and auditing tools, such as the development of data-mining capabilities, training of GCPC program administrators and cardholders has also been enhanced. These improvements to GCPC program training represent attempts to implement preventive measures to complement the more reactive tools designed to help identify fraud and card misuse after it occurs.

From our examination of internal control theory, Lieutenant Colonel Darling and I concluded additional potential exists to further improve the GCPC program internal control environment. As discussed by Joseph T. Wells, founder of the Association of Certified Fraud Examiners, in his 1997 book, Occupational Fraud and Abuse, there are identifiable factors common to fraud within organizations. Wells argued that for fraud to occur there must exist three legs of support for a fraud triangle; those legs consist of incentive, opportunity, and rationalization.

Incentive means the perpetrator of the fraud has something to gain; not all such gains need be monetary. As is intuitively obvious, the opportunity to commit fraud must exist, or fraud is impossible for an individual no matter how much he might desire to steal from his organization. And finally, particularly for otherwise honest individuals, the ability to rationalize an illicit action acts as a critical enabler of fraud. The fraud triangle is depicted in Figure 3.

9. GAO Testimony Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, p. 2.

According to the fraud triangle theory, one way to help ensure an adequate internal control environment is to limit an individual's ability to rationalize illicit activities. By lessening the ability of an individual to convince himself that his actions are justifiable (due to perceived urgency of need, that he deserves or requires an item despite existing guidance or instructions to the contrary, that an action can be construed as within the larger meaning of those instructions, etc.), an organization should be able to lower the probability that members of that organization will commit fraud against it.

Undoubtedly, because the GCPC program provides individuals access to large amounts of government credit, an incentive to commit fraud is inherent in the program. Likewise, cardholders and program administrators have numerous opportunities to steal from the government or otherwise misuse GCPC program cards. The potential for fraudulent use of cards ranges from a cardholder purchasing an item for his personal use and hoping it will not be noticed by the AO or APC during the bill reconciliation process to cardholders and administrators colluding to make split purchases (exceeding the \$2,500 per purchase cap by splitting the purchase into two or more separate purchases).

Although the potential for fraud in the GCPC program thus will always exist, automated control measures (such as restrictions on where purchases can be made), verification requirements, and receipt and audit procedures can largely suffice to identify illicit card use. These types of controls, coupled with the purchasing limits in place on individual cards, help ensure fraud will be prevented or identified, as well as monetarily limiting any one individual's ability to defraud the government.

Rationalization

Many government employees, and many Marines, who have made illicit purchases with their GCPC cards or who have ignored existing, mandatory internal controls and established internal control processes, would not consider themselves thieves. Whether purchasing a sandwich at Subway or bedding and towels for a visiting foreign military officer (both examples of GCPC card misuse documented in the Marine Corps' semi-annual review of the GCPC program for the first half of FY-03), otherwise trusted and diligent government employees who improperly used their government purchase cards often did so for items which involved very low dollar amounts or did not directly benefit themselves. It is likely they saw those purchases as not truly representing fraud against the government of the United States.

With an incentive and an opportunity, an individual need only be able to rationalize a questionable purchase to significantly enhance his potential to commit fraud or otherwise misuse a GCPC program card. Even for those making comparatively large illicit purchases, there is likely to exist at the root of the fraud a rationalization that at the time, in the eyes of the purchaser, justified the transaction.

Our ability to see the illegitimacy of those rationalizations (and the fact that the ability to rationalize a wrongful action does not make it justifiable) is not the point. The point is that the ability to rationalize card fraud, misuse, and abuse contributes to the poor internal control environment existing in the GCPC program. The recommendations offered in the remainder of this article are designed to counter the ability of those administering the GCPC program, particularly cardholders, to rationalize wrongful use of GCPC program cards.

Recommendations to Improve the GCPC Program

The analysis contained within the NPS thesis upon which this article is based led the authors of that thesis to recommend four changes to the GCPC program as it is currently administered within the Marine Corps. Three of those recommendations were designed to directly combat the potential for rationalization of illicit card use the authors believed inherent in the current program; those three recommendations are encapsulated in the following paragraphs. Although these recommendations have no potential to prevent willful theft by illicit use of GCPC program cards, they can help lessen the potential for GCPC program cardholders and administrators to rationalize illicit use of the cards. These recommendations are to: convert the GCPC cards from individually named credit cards to unit cards with personalized numbers; to change the appearance of the cards; and to provide electronic receipts of all cardholder transactions daily to AOs and APCs.

GCPC program purchase cards are issued with the cardholder's name embossed on them as an internal control measure. Since only the individual cardholder can make purchases with the card (as only his/her name is on it), it is relatively simple to establish who made a questionable purchase. However, since the cards are similar in appearance to non-government credit cards and since the individual's name appears on the card, there is a risk that an individual may mistake the GCPC card for his/her personal credit card or be able to rationalize illicit use of the GCPC program card as it is "his/hers" because it bears his/her name. Particularly for

individuals with little experience in financial management prior to entering the service, the issuance of a credit card with their name on it, which looks strikingly similar to a personal credit card, may be providing them an undeserved sense of entitlement to the use of the card. It is also unnecessary.

The DoN's current service contract with Citibank does not limit the structure of its GCPC card accounts, meaning whether the cards are issued to individuals or to organizations is determinable by the DoN. By issuing the GCPC program cards with unit identifiers instead of personal names embossed on the front of the cards while associating card numbers to individual cardholders, the DoN can negate much of the potential for rationalization inherent in the current program while maintaining a high level of card use accountability. To accomplish this would require modification to the current GCPC cards.

The recommendation contained in the NPS thesis for a revised GCPC unit card is depicted in Figure 5. The card would still be issued directly from Citibank to the cardholder but would not bear the cardholder's name. For accountability and to establish pecuniary liability to the cardholder, the last four digits of the card would be used to identify the individual cardholder. APCs and HAs would have increased interest in ensuring detaching cardholders returned their cards and had their accounts deactivated as the cards would be directly associable to the unit instead of to the individual cardholders. As is true of the program as currently administered, the cardholder would have sole access to his GCPC card while serving as a cardholder, yet one potential source of the ability of a cardholder to rationalize illicit purchases (believing the card to be his because his name is on it) would be eliminated.

According to the Camp Pendleton, CA, APC, cardholders had sometimes explained that their illicit GCPC purchases were simple mistakes made because their GCPC program cards looked too much like their other, personal credit cards. Changing the GCPC program card appearance to make it more distinctive is an obvious solution to this type of confusion experienced by cardholders. The current GCPC program card, depicted in Figure 4, is very visually appealing and contains the sentence "For Official US Government Purchases Only" in faint, extremely small print under a large heading reading "United States of America." In addition to GCPC cardholder confusion, vendors seeing the large "VISA" symbol and the embossed cardholder's name can themselves easily overlook the tiny official purchase warning.

Although one benefit of the current appearance of the GCPC card is likely its unquestioned acceptance by commercial vendors as it looks largely like any other personal credit card, the

card's appearance can be modified to eliminate any cardholder perception that the card isn't as "official" as it is in reality. As depicted in Figure 5, a redesigned GCPC program card, while still visually appealing, would bear the issuing unit's name instead of the individual cardholder's name and a statement in large print **"FOR OFFICIAL US GOVERNMENT PURCHASES ONLY, CARDHOLDER VIOLATIONS SUBJECT TO 31 U.S.C 3528."** A GCPC cardholder should find it much more difficult to mistake such a redesigned card for a personal credit card or to rationalize unauthorized purchases.

Lastly, AOs and APCs could be provided electronic receipts of all cardholder transactions on a daily basis instead of just at the end of the billing cycle (in the monthly billing statement from Citibank). As stated in the 2002 DoD Charge Card Task Force Final Report, "...the most critical management controls in the purchase card program are the monthly review and approval of the cardholder's statement by the approving official..."¹⁰

Citibank currently provides an on-line capability to data-mine account transaction activity for all GCPC accounts and APCs and AOs are required to review, and AOs to certify, their cardholders' accounts on a monthly basis. Yet technology could easily make review of account statuses a daily activity for APCs and AOs by automatically providing them an account summary on a daily versus monthly basis.

APCs and AOs, screening their cardholder transactions daily, would no longer face the deluge of end of billing cycle verifications which presently confront them. This monthly deluge, along with the requirement to quickly complete the verification and certification processes, can tempt GCPC program administrators to perform a less than detailed review of their cardholders' monthly transactional activities. Even the most diligent auditor is more likely to miss identifying a questionable transaction when faced with reviewing an entire month's activities by all his cardholders, while also trying to complete his review quickly to ensure his certification is submitted on time. The necessity to review transactions daily would also add a level of discipline to the present review and certification process. Since the requirement to review and certify all cardholder transactions already exists, daily review only disciplines, instead of adding to, the completion of current requirements.

Additionally, cardholders, well aware that each transaction would be reviewed by both the AO and the APC the day the purchase was made, would be less able to rationalize

9. DoD Charge Card Task Force Final Report, p. 2-4.

questionable purchases. The knowledge that any such purchases would be more likely to be immediately identified would help negate the potential for cardholders to self-justify illicit card use by believing such use to be unlikely to be detected.

Conclusion

Fraud may not be fully preventable in any procurement process or program. Some incentive will always exist to steal, as will some opportunity to commit fraud. Likewise, even well designed internal controls have little impact in preventing fraud if they are not effectively implemented. In the GCPC program, the internal controls thus far in use to limit fraud, waste, and abuse with program cards may be better at detecting fraud and misuse after it occurs than in preventing it in the first place. Certainly the types of difficulties in internal control implicit in the opening quote to this article indicate there is room to improve in prevention of fraud within the GCPC program.

Breakdowns in internal controls are both extraordinarily easy to envision and exceedingly difficult to prevent. For example, if an AO, pressed for time, does not actually review all the transactions for a particular cardholder and instead simply certifies the invoice to ensure it is submitted on time, there exists a potential for fraud to escape detection. If a unit, due to personnel limitations for instance, does not really separate the duties of purchasing, receipting for, and inventorying purchased items, the GCPC cardholder making the purchase has ample opportunity to defraud the government.

As long as an incentive and the potential to commit fraud or other card misuse exists within the GCPC program, the key to prevention is likely to be found in limiting the ability of individuals to rationalize illicit purchases. In recent years, much has been done to limit the opportunity for individuals to perpetrate fraud within the GCPC program and to improve the ability of program administrators to detect fraud or card misuse when it occurs; however, those initiatives can completely eliminate neither the incentive nor the opportunity for fraud and card misuse. If they could, they would have already accomplished that purpose. By implementing the recommendations contained within this paper, the Marine Corps and other organizations can limit the ability of individuals to rationalize illicit use of GCPC program cards and improve the GCPC program internal control environment.

(Amounts calculated in thousands)

FY 03 DoD Purchase Card Usage US Bank and Citibank					
	Total Accounts		Fiscal Year thru 30 Sep 03		TOTAL
Agency	B/O	C/H	Sales	Transactions	Rebates
Navy (17)	4,823	19,807	\$1,853,181	2,539	\$4,436
Army (21)	26,202	66,922	\$3,026,240	4,510	\$19,837
Air Force (57&58)	19,294	47,437	\$1,757,483	3,018	\$14,039
Defense Agencies (97)	3,108	7,207	\$ 599,072	666	\$2,769
Totals	53,427	141,373	\$7,235,977	10,735	\$ 36,082

Figure 1. FY-03 DoD Purchase Card Usage. (From: <http://purchasecard.saalt.army.mil//03metrics.htm>, 31 Oct 2003)

CHAPTER 2: MANAGING COMMAND PURCHASE CARD PROGRAMS

Purchase Card Hierarchy Diagram.

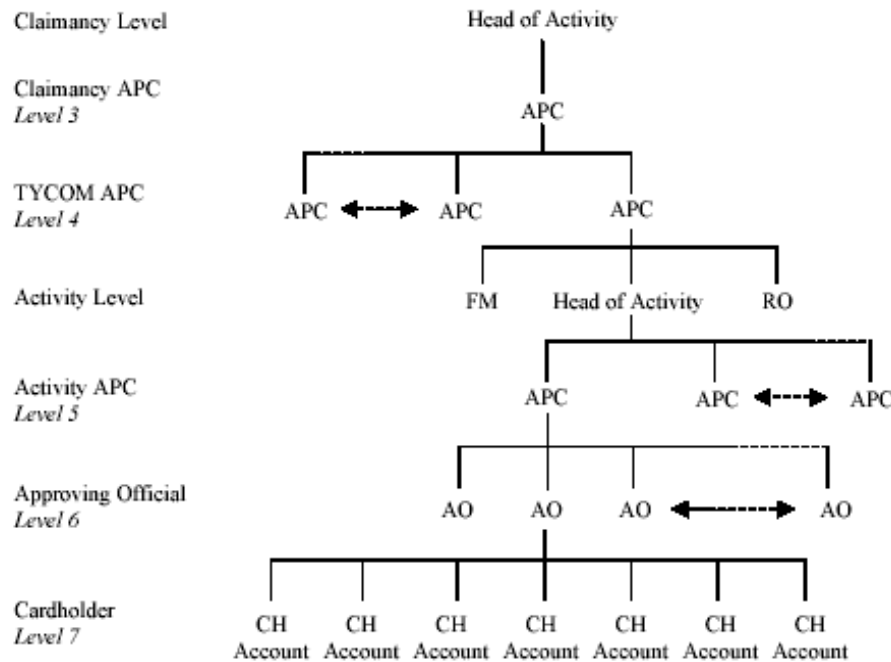


Figure 2. Purchase Card Hierarchy Diagram. (From: DoN EBUSOPSOFFINST 4200.1A, p. 13)

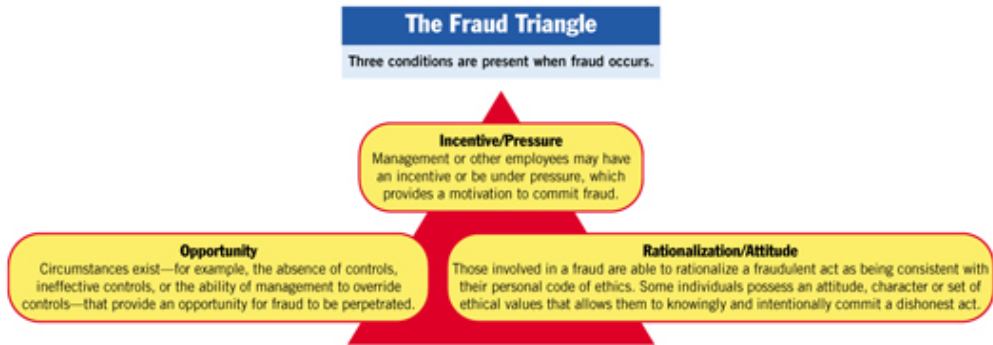


Figure 3. The Fraud Triangle. (From: <http://www.aicpa.org/pubs/jofa/jan2003/ramos.htm>)

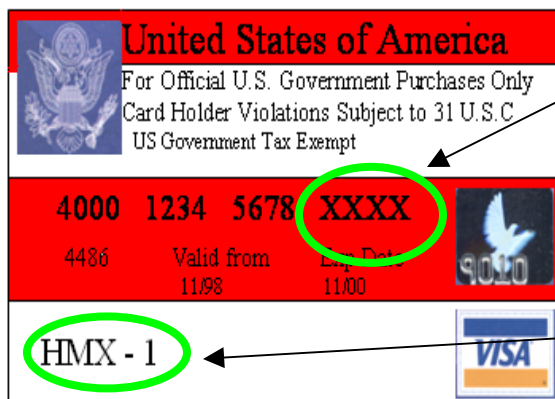
The GCPC program card of today:



The current card looks like a personal credit card and bears the cardholder's name

Figure 4.

The GCPC program card of tomorrow:



These last four digits would be different for every user; the numbers would identify the card's authorized user

The unit name would replace the individual cardholder's name here

Figure 5.

LIST OF SELECTED REFERENCES

1. Logistics Branch, Purchase Card Response Format Semi-annual Review, 4 June 2003, prepared by Major Chester McMillon
2. Department of the Navy, E-Business Operations Office Instruction 4200.1A, September 2, 2003
3. Department of Defense, Comptroller, Charge Card Task Force Final Report, June 27, 2002, available from World Wide Web @ http://www.dod.mil/comptroller/Charge_Card_TF_Final.pdf
4. "DoD Moves To Improve Charge Card Programs" Defense Link, (27 Jun. 2002); available from World Wide Web @ http://www.defenselink.mil/news/Jun2002/b06272002_bt332-02.html
5. Interview with Denise Parks, Agency Program Coordinator, Marine Corps Air Station Miramar, 21 August 2003
6. House Committee on Government Reform, *GAO Testimony Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations*, (July, 2001). Purchase Cards, Control Weaknesses Leave Two Navy Units Vulnerable to Fraud and Abuse, Statement of Gregory D. Kutz Director, Financial Management and Assurance Statement of Robert H. Hast, Managing Director, Office of Special Investigations
7. Occupational Fraud and Abuse, Joseph T. Wells, 1997, Obsidian Publishing Company, Inc. Austin, Texas